| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-6** | SECURITY FUNCTIONALITY VERIFICATION | |
| **SI-6.1**  **SI-6.1.1**  **SI-6.1.2**  **SI-6.1.3**  **SI-6.1.4**  **SI-6.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions;* 2. *the organization defines for periodic security function verification, the frequency of the verifications;* 3. *the organization defines information system responses and alternative action(s) to anomalies discovered during security function verification;* 4. *the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and* 5. *the information system responds to security function anomalies in accordance with organization-defined responses and alternative action(s).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Security function verification capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-3, CM-4, CM-6, RA-5, SA-4, SA-5, SA-11  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **SI-6.1.1.1** | | **Examine** system and information integrity policy, procedures addressing security function verification, security plan, or other relevant documents; [*reviewing*] for the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions. |
|  | |  |
| **SI-6.1.2.1** | | **Examine** system and information integrity policy, procedures addressing security function verification, security plan, or other relevant documents; [*reviewing*] for the frequency of periodic security function verification. |
|  | |  |
| **SI-6.1.3.1** | | **Examine** system and information integrity policy, procedures addressing security function verification, security plan, or other relevant documents; [*reviewing*] for information system responses and alternative action(s) to anomalies discovered during security function verification. |
|  | |  |
| **SI-6.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to verify the correct operation of security functions in accordance with the conditions identified in SI-6.1.1.1 and in accordance with the frequency identified in SI-6.1.2.1 (if periodic verification). |
| **SI-6.1.4.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-6.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-6.1.4.1. |
| **SI-6.1.4.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-6.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SI-6.1.5.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to respond to security function anomalies in accordance with the responses and alternative actions identified in SI-6.1.3.1. |
| **SI-6.1.5.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-6.1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-6.1.5.1. |
| **SI-6.1.5.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-6.1.5.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-6(1)** | SECURITY FUNCTIONALITY VERIFICATION |
| **SI-6(1).1**  **SI-6(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system provides notification of failed automated security tests.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; automated security test results; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing alerts and/or notifications for failed automated security tests]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-3, CM-4, CM-6, IR-4, IR-6, SA-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-6(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to provide notification of failed automated security tests. |
| **SI-6(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-6(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-6(1).1.1.1. |
| **SI-6(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-6(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-6(2)** | SECURITY FUNCTIONALITY VERIFICATION |
| **SI-6(2).1**  **SI-6(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system provides automated support for the management of distributed security testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting the management of distributed security function testing]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-3, CM-4, CM-6, SA-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-6(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to provide support for the management of distributed security testing. |
| **SI-6(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-6(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-6(2).1.1.1. |
| **SI-6(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-6(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-6(3)** | SECURITY FUNCTIONALITY VERIFICATION |
| **SI-6(3).1**  **SI-6(3).1.1**  **SI-6(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies organizational officials with information security responsibilities designated to receive the results of security function verification; and* 2. *the organization reports the results of security function verification to designated organizational officials with information security responsibilities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security functionality verification responsibilities; organizational personnel with information security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-7, CM- 4, IR-4, IR-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-6(3).1.1.1** | **Examine** system and information integrity policy, procedures addressing security function verification, security plan, or other relevant documents; [*reviewing*] for the organizational officials with information security responsibilities designated to receive the results of security function verification. |
|  |  |
| **SI-6(3).1.2.1** | **Examine** system and information integrity policy, procedures addressing security function verification, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to report the results of security function verification to the designated organizational officials identified in SI-6(3).1.1.1. |
| **SI-6(3).1.2.2** | **Examine** an agreed-upon [*basic*] sample of security function verification reports, emails, or other relevant documentation generated to report results of security function verification to the organizational officials identified in SI-6(3).1.1.1; [*reviewing*] for evidence that the measures identified in SI-6(3).1.2.1 are being applied. |
| **SI-6(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational officials identified in SI-6(3).1.1.1; conducting [*basic*] discussions for further evidence that the measures identified in SI-6(3).1.2.1 are being applied. |